ABSTRACT OF THE DISCLOSURE

A malware detection system and method for determining whether an executable script is malware is presented. The malware detection system determines whether the executable script is malware by comparing the functional contents of the executable script to the functional contents of known malware. In practice, the executable script is obtained. The executable script is normalized, thereby generating a script signature corresponding to the functionality of the executable script. The script signature is compared to known malware script signatures in a malware signature store to determine whether the executable script is malware. If a complete match is made, the executable script is considered to be malware. If a partial match is made, the executable script is considered to likely be malware. The malware detection system may perform two normalizations, each normalization generating a script signature which is compared to similarly normalized known malware script signatures in the malware signature store.